AP
IFW

Attorney Dkt.
P56352

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Young-Hyun Kang

Serial No.:	09/834,901	Examiner:	C. Zhong
Filed:	16 April 2001	Art Unit:	2152

For: METHOD FOR MANAGING ALARM INFORMATION IN A NETWORK MANAGEMENT SYSTEM

Appeal No.________________

Mail Stop Appeal Briefs - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

ATTENTION: Board of Patent Appeals and Interferences

<u>CORRECTED APPELLANT'S BRIEF (37 CFR §41.37)</u>

<u>Paper No. 14</u>

In response to the Notification of Non-Compliant Appeal Brief mailed on 18 October 2006 (Paper No. 20061005), Appellant submits the Corrected Appellant's Brief. In this Corrected Appellant's Brief, (1) the status of claims under appeal for Claims Appendix is listed and (2) Appellant's undersigned attorney has signed all three (3) copies of the brief. No new matter is inserted.

This brief is in furtherance of the Notice of Appeal filed in this case on 28 April 2006.

No fee is incurred by filing of this Corrected Appellant's Brief.

Folio: P56352
Date: 10/30/06
I.D.: REB/MDP

CERTIFICATE OF FACSIMILE TRANSMISSION

I hereby certify that, on <u>30 October 2006,</u> this correspondence is being facsimile transmitted to the U.S. Patent & Trademark Office **(Facsimile No. 571-273-8300)**

Total 27 sheets

F. Watanabe
For Robert E. Bushnell
Reg. No. 27,774

APPEAL BRIEF

I. STATEMENT OF REAL PARTY IN INTEREST

Pursuant to 37 CFR §41.37(c)(1)(i) the real party in interest is:

SamSung Electronics Co., Ltd.
416 Maetan-dong, Yeongtong-gu,
Suwon-si, Gyeonggi-do,
Republic of Korea

II. RELATED APPEALS AND INTERFERENCES

Pursuant to 37 CFR §41.37(c)(1)(ii), there are no appeals nor interferences known to the Appellant, the Appellant's legal representative, or the Assignee (real party of interest) which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

III. STATUS OF CLAIMS

Claims 1-14 are finally rejected, such rejection being appealed herein.

IV. STATUS OF AMENDMENTS FILED AFTER FINAL REJECTION

No Amendment has been filed.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Claim 1. *A method for managing alarm information in a network management system, comprising the steps of:*

receiving alarm information generated from any of a plurality of network elements; Paragraph [0030]; Figs. 3 and 5; step 502, the alarm daemon processor 304 of network management system 300 receives any the alarm information generated from network elements 308, 310, 312 connected via the communications network of server 306.

determining whether or not said alarm information corresponds to a logical alarm; Paragraph [0032]; Figs. 3 and 5; step 504, the network management system 300 analyzes the alarm data format to determine at step 504 whether the nature of the alarm corresponds to a logical error or a physical error. If the alarm generated from a certain network element is determined to correspond to a physical error, like loss of signal (LOS), alarm indication signal (AIS), loss of frame (LOF), loss of pointer (LOP), etc., rather than a logical alarm like loss of link (LOS), poor quality of signal (QOS), etc., the network management system proceeds to step 506 to simply parse the data format of the received alarm information for storage into the database 302.

determining the location of the network element generating the alarm information, when it is determined that the alarm information corresponds to a logical alarm; Paragraph [0033]; Figs. 3 and 5; step 508, if the alarm is determined to correspond to a logical error, the network management system 300 proceeds to step 508 to retrieve the alarm location (dn).

searching a database to determine whether said database already has said alarm information stored therein, according to the location of the network element generating the alarm information; Paragraph [0033]; Figs. 3 and 5; steps 510 and 512, it proceeds to step 510 to identify the destination information (DPID) by the VPI/VCI (virtual path identifier/ virtual channel identifier) of the subscriber connection information corresponding to the alarm location (dn); and Paragraph

[0035] Then, the network management system 300 searches, at step 512, the database 302 to determine if it already includes the same information, *i.e.,* as the present alarm information. That is, at step 512, the alarm information is analyzed to detect a positional value, event type and the destination information by the VPI/VCI of the subscriber connection information corresponding to the alarm location (dn) to determine whether the alarm information corresponds to alarm information already received and stored in database 302. This is to avoid storing, into the database 302, redundant logical alarm information recurring at the same subscriber location, thus both economizing the storage capacity of the database and simplifying a searching process.

storing said alarm information when it is determined that said database does not have said alarm information already stored therein; Paragraph [0038]; Figs. 3 and 5; step 516, if the alarm information has not been stored in the database 302, the network management system 300 proceeds to step 516 to convert the present alarm information through a database application interface (DBAPI: not shown) into the database data format to be recorded as new alarm information in the alarm table of the corresponding network element.

increasing a count value representing a number of times in which the same alarm information has been generated, without redundantly storing said alarm information into said database, when it is determined that said alarm information is already stored in said database; Paragraph [0035]; Figs. 3 and 5; step 514, if the same alarm information has already been stored in the database 302, the network management system 300 proceeds to step 514 to increase the count representing the number of recurrences of the same alarm instead of repeatedly storing the alarm information into the database 302.

storing the increased count value at a position corresponding to said alarm information already stored in said database; Paragraph [0037]; Figs. 3, 5 and 8; step 514; Fig. 8, Fig. 8 shows a screen displaying the alarm information when storing the increased count representing the number of recurrences of the same alarm into the database 302. The alarm information table additionally includes the subscriber statistics item recording the number of recurrences of the logical alarm so as both to economize the storage capacity of the database 302 and to simplify the searching process, compared to the table as shown in Fig. 2.

Claim 8. *A method for managing alarm information in a network management system connected to a plurality of subscribers at a plurality of network elements, comprising the steps of:*

driving an alarm daemon processor when said network management system is powered on; Paragraph [0030]; Figs. 3 and 5; step 500, the network management system 300, while turned on, works the alarm daemon processor 304.

receiving, via said alarm daemon processor, alarm information generated from at least one of said network elements; Paragraph [0030]; Figs. 3 and 5; step 502, the alarm daemon processor 304 of network management system 300 receives any the alarm information generated from network elements 308, 310, 312 connected via the communications network of server 306.

determining whether said alarm information is due to a logical error or a physical error in the network element generating the received alarm information; Paragraph [0032]; Figs. 3 and 5; step 504, the network management system 300 analyzes the alarm data format to determine at step 504 whether the nature of the alarm corresponds to a logical error or a physical error. If the alarm

generated from a certain network element is determined to correspond to a physical error, like loss of signal (LOS), alarm indication signal (AIS), loss of frame (LOF), loss of pointer (LOP), etc., rather than a logical alarm like loss of link (LOS), poor quality of signal (QOS), etc., the network management system proceeds to step 506 to simply parse the data format of the received alarm information for storage into the database 302.

determining the location of the network element generating the alarm information, when it is determined that the alarm information is due to a logical error; Paragraph [0033]; Figs. 3 and 5; step 508, if the alarm is determined to correspond to a logical error, the network management system 300 proceeds to step 508 to retrieve the alarm location (dn).

searching a database to determine whether said database already has said alarm information stored therein, according to the location of the network element generating the alarm information; Paragraph [0033]; Figs. 3 and 5; steps 510 and 512, it proceeds to step 510 to identify the destination information (DPID) by the VPI/VCI (virtual path identifier/ virtual channel identifier) of the subscriber connection information corresponding to the alarm location (dn); and Paragraph [0035] Then, the network management system 300 searches, at step 512, the database 302 to determine if it already includes the same information, *i.e.,* as the present alarm information. That is, at step 512, the alarm information is analyzed to detect a positional value, event type and the destination information by the VPI/VCI of the subscriber connection information corresponding to the alarm location (dn) to determine whether the alarm information corresponds to alarm information already received and stored in database 302. This is to avoid storing, into the database 302, redundant logical alarm information recurring at the same subscriber location, thus both economizing

the storage capacity of the database and simplifying a searching process.

storing said alarm information when it is determined that said database does not have said alarm information already stored therein; Paragraph [0038]; Figs. 3 and 5; step 516, if the alarm information has not been stored in the database 302, the network management system 300 proceeds to step 516 to convert the present alarm information through a database application interface (DBAPI: not shown) into the database data format to be recorded as new alarm information in the alarm table of the corresponding network element.

increasing a count value representing a number of times in which the same alarm information has been generated, without redundantly storing said alarm information into said database, when it is determined that said alarm information is already stored in said database; Figs. 3 and 5; step 514, if the same alarm information has already been stored in the database 302, the network management system 300 proceeds to step 514 to increase the count representing the number of recurrences of the same alarm instead of repeatedly storing the alarm information into the database 302.

storing the increased count value at a position corresponding to said alarm information already stored in said database. Paragraph [0037]; Figs. 3, 5 and 8; step 514; Fig. 8, Fig. 8 shows a screen displaying the alarm information when storing the increased count representing the number of recurrences of the same alarm into the database 302. The alarm information table additionally includes the subscriber statistics item recording the number of recurrences of the logical alarm so as both to economize the storage capacity of the database 302 and to simplify the searching process, compared to the table as shown in Fig. 2.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. Whether claims 1-14 are allowable under 35 U.S.C. §112, first paragraph.

B. Whether claims 1-14 are allowable under 35 U.S.C. §112, second paragraph.

C. Whether claims 1-14 are patentable under 35 U.S.C. §103 over the combination of Harris (US 5,946,373) and Joyce (US 4,195,343).

VII. ARGUMENTS

A. The specification has been objected to and claims 1-14 have subsequently been rejected under 35 U.S.C. §112, first paragraph. The applicant respectfully traverses this rejection for the following reason(s).

The Examiner errs in holding the disclosure to be a non-enabling disclosure based on the phrases "logical alarm" and "physical alarm" **(a.k.a.: hardware alarm; analog alarm; real alarm)**. The Examiner has indicated that the Applicant has failed to clearly define the differences between the two terms. It should be noted that these terms are well known in the art of network communication.

Basic definitions include:

Real alarm: A real alarm is a transaction that represents a physical (hardware) alarm that later requires to be cleared;

Logical alarm: A logical alarm is any transaction event (with the exception of alarm

acknowledges) that does not relate to a hardware state.

Note that the standard for providing an enabling disclosure is determined by "one of ordinary skill in the art." The various terms that the Examiner has issues with are well known in the art. The standard is not based what the Examiner can or cannot understand. The Examiner is not one of ordinary skill in the art. The Examiner is only assumed to have knowledge of the art or the ability to review the known art and understand the principles thereof.

The Examiner points to the terms "Loss of Signal" and "Loss of Link" and indicates that either one could lead to the other. In network communications, however, it is well known that the detection of Loss of Signal is different from the detection of Loss of Link. For example, the OSI (Open Systems Interconnections) standard divides telecommunications into seven layers. One layer (Layer 1) is known as the "Physical Layer" and another layer (Layer 2) is known as the "Data Link Layer".

Each layer is monitored, and alarms created based on errors detected in the physical layer (layer 1) will result in the generation of a **physical alarm**. The features looked for **are well known in the art**, such as loss of signal (LOS), loss of frame (LOF) or loss of pointer (LOP).

Alarms created based on errors detected in the data link layer (layer 2) result in the generation of a **logical alarm**. The features looked for **are also well known in the art**, such as loss of link (LOS), or poor quality of signal (QOS).

In paragraph [0032] of the specification, it is definitely disclosed so that a logical error related to a logical alarm and a physical error related to a physical alarm are discerned from each other, thus those of ordinary skill in the art can easily understand what a logical alarm and a physical

is based on the original specification.

The specification defines a **logical alarm** as one of, for example, a loss of link (LOL) or a poor quality of signal (QOS), and defines an alarm **(physical alarm)** corresponding to physical information (error) as one of, for example, loss of signal (LOS), alarm indication signal (AIS), loss of frame (LOF), or loss of pointer (LOP).

More specifically, amended paragraph [0032] states:

> Accordingly, the network management system 300 analyzes the alarm data format to determine at step 504 whether the nature of the alarm corresponds to a logical error or a physical error. If the alarm generated from a certain network element is determined to correspond to a physical error, like loss of signal (LOS), alarm indication signal (AIS), loss of frame (LOF), loss of pointer (LOP), etc., rather than a logical alarm like loss of link (LOL), poor quality of signal (QOS), etc., the network management system proceeds to step 506 to simply parse the data format of the received alarm information for storage into the database 302.

Therefore, since the phrases "physical alarm" and "logical alarm" and the differences there between are well known in the art, the rejection is deemed to be in error and should not be sustained.

B. Claims 1-14 were rejected under 35 U.S.C. §112, second paragraph based upon a number of deficiencies kindly noted by the Examiner. The Applicant respectfully traverses this rejection for the following reason(s).

a) The Examiner errs is holding that the phrase "logical alarm", claim 1, lines 4 and 6, is not supported by the specification.

Amended paragraph **[0032]** discloses:

> Accordingly, the network management system 300 analyzes the alarm data format to determine at step 504 whether the nature of the alarm corresponds to a **logical error** or a physical error. If **the** **<u>alarm</u>** generated from a certain network element is determined to **correspond to a physical error**, like loss of signal (LOS), alarm indication signal (AIS), loss of frame (LOF), loss of pointer (LOP), etc., rather than a **logical alarm** like loss of link (LOL), poor quality of signal (QOS), etc., the network management system proceeds to step 506 to simply parse the data format of the received alarm information for storage into the database 302. (emphasis added)

Accordingly, the specification, and in particular, paragraph **[0032]** uses both terms "logical error" and "logical alarm" and defines how these terms are related.

b) The Examiner errs is holding that the phrase "alarm information corresponding to a logical alarm" (*alarm information corresponds to a logical alarm*: claim 1, line 4) is not understood . The Examiner errs in stating that " 'logical' may refer to the type of errors that contribute to alarm information, but not to the alarm."

Clearly, if the error type is a logical error, and such errors generate an alarm, then the alarm can be deemed a *logical alarm*, especially when paragraph **[0032]** of the specification relates logical errors and logical alarms. Additionally, the Applicant can be his own lexicographer and as long as the terminology is defined by the specification, then there is no error in its use.

As noted with respect to the rejection under §112, first paragraph, the term logical alarm is well known in the art and the specification does not include a definition contrary to what is already known in the art.

c) The Examiner indicates that the phrase "alarm information does not correspond to a logical

alarm" (*alarm information corresponds to a logical alarm*: claim 4, line 3) is not understood, holding that it "is unclear what other type of alarm information can exist or how to differentiate between them."

The purpose of the claim is to set forth the invention in a clear manor in light of the specification. Claims are not to be read in a vacuum. It is the purpose of the specification, not the claims, to define what other type of alarm information can exist and how to differentiate between them. The specification clearly defines the different types of alarms that can exist. It is well known in the art how to differentiate between different types of alarms.

Besides, claim 1 calls for *determining* <u>*whether or not*</u> *said alarm information corresponds to a logical alarm*. Therefore, it only matters whether the alarm information is a logical alarm. If it is not a logical alarm, in this instance, then it can be any type of other alarm. The claim, at this point, is only concerned with logical alarms.

d) The Examiner indicates that the phrases "logical error" and "physical error" of claim 8, lines 6 and 9, and claim 1, line 3, are not understood, and more specifically the Examiner fails to understand how an error may be designated as logical or physical.

It has been shown that it is well known in the art what is meant by "logical error" and "physical error" ("logical alarm" and "physical alarm") and that it is well known by those of ordinary skill in the art how to differentiate between them.

Each of the issues raised by the Examiner have been shown to be easily understood by one

of ordinary skill in the art and/or well defined by the specification. Accordingly, the rejection is deemed to be in error should not be sustained.

C. Claims 1-14 were rejected under 35 U.S.C. §103(a) as being obvious in view of Harris (US 5,946,373) and Joyce (US 4,195,343). The applicant respectfully traverses this rejection for the following reason(s).

Claims 1 and 8

The present invention relates to a network management system for optimizing a database which stores alarm information generated from a plurality of network elements in order to manage those network elements.

In particular, when an alarm is received it is first determined whether the alarm is a logical alarm or based on physical information. Then the network element generating the alarm is determined and a database is maintained to record the occurrence if it is a logical alarm as opposed to physical information. Each time a particular network element generates an already recorded alarm occurrence, a counter is increased with the increased count being recorded instead of recording the alarm event again.

The specification defines a logical alarm as one of, for example, a loss of link (LOL) or a poor quality of signal (QOS), and defines an **alarm** corresponding to a **physical error** as one of, for example, **loss of signal (LOS)**, alarm indication signal (AIS), loss of frame (LOF), or loss of pointer (LOP). See paragraph [0032].

Harris' invention also relates to a network management system for optimizing a database which stores alarm information generated from a plurality of network elements in order to manage those network elements.

There does not appear to be any disclosed determination of whether or not the alarm information corresponds to a logical alarm.

Note in col. 1, lines 61-65, Harris mentions "when a failure occurs on a circuit, the equipment closest to the failure detects the fault ("loss of signal", for example), reports the fault, and propagates an alarm indicator signal in the "downstream" direction on the affected circuit." Accordingly, at least one fault in Harris is defined as a 'loss of signal," which has been defined by the present invention as a physical error instead of a logical error.

In col. 4, lines 11-14, Harris discloses that only certain alarm messages are extracted and analyzed, *i.e.*, "This invention contains an interface, shown in FIG. 2A, to the message reception process to extract only certain selected fault alarm messages as indicated in step 201. That is, those fault alarms <u>indicating a circuit or trunk traffic outage</u>, plus the messages that indicate that such a fault condition has now "cleared".

Accordingly, Harris is only concerned with physical errors and thus, physical alarms.

That is, Harris only checks for a circuit or trunk outage. Harris does not look for the cause of the outage, such whether it was due to a loss of link (LOL) or a loss of signal (LOS).

Therefore, there is clearly no method of *determining whether or not said alarm information <u>corresponds to a logical alarm</u>* (claim 1). As mentioned above, Harris is only concerned with physical alarms, and thus has no desire to determine whether or not alarm information corresponds

to a logical alarm. That is, Harris only teaches determining whether or not alarm information corresponds to a physical alarm.

Note that the terms "logical alarms" and "physical alarm" are not open to unreasonable interpretation, that is, interpretations outside the bounds of the Applicant's disclosure and what is well known in the art. The difference between "physical alarms" and "logical alarms" are well established in the art. Harris's circuit and trunk traffic are physical (hardware) features of a network, and therefore correspond only to "physical errors" and related "physical alarms."

The Examiner does not apply Joyce as a teaching of the foregoing feature noted as lacking in Harris. Accordingly, the combination of Harris and Joyce fails to make obvious the feature of *determining whether or not said alarm information corresponds to a **logical** alarm.*

In the final rejection, pages 10-11, the Examiner has disregarded what is well known in the art to be a logical error as opposed to a physical error. The Examiner also appears to disregard the Applicant's specification which defines logical errors/logical alarms and physical error/physical alarms, and in particular, paragraph [0032] even after the Examiner repeated paragraph [0032].

In analyzing the scope of a claim, office personnel must rely on Applicant's disclosure to properly determine the meaning of the terms used in the claim. *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 980, 34 USPQ2d 1321, 1330 (Fed. Cir. 1995); *In re Cruciferous Sprout Litigation*, 301 f.3d 1343, 1348, 64 USPQ2d 1202, 1205 (Fed Cir. 2002) (citing *Intervet America Inc. v. Kee-Vet Labratories Inc.*, 12 USPQ2d 1474, 1476 (Fed. Cir. 1989). We do recognize that the Examiner has held the disclosure to be "not enabling," such holding being traversed above.

The Examiner has unreasonably chosen to define at least one of Harris' physical alarms as a logical alarm. Harris discloses in col. 2, lines 41-42 that "Each alarm represents a specific fault detected on a particular piece of equipment." Accordingly, since each "particular piece of equipment" is known in the art to be a physical element, a piece of hardware, then the fault on a particular piece of equipment can only be deemed a physical error and thus the alarm generated in response thereto is deemed to be a physical alarm.

Absent knowledge of the present invention, one of ordinary skill in the art would have deemed a specific fault detected on a particular piece of equipment disclosed in Harris to constitute a physical error and thus the alarm generated in response thereto is deemed to be a physical alarm.

In col. 2, lines 25-39 (cited by the Examiner), Harris clearly discusses "equipment alarms" and using network circuit topology to correlate the equipment alarms and as a result infers a trunk outage from circuit alarms, even if no fault has been reported on the trunk; confirming that a reported trunk fault is actually causing a traffic outage if the contained circuits are also in alarm; correlating transmission system trunk outages that share the same path (e.g., fiber optic pairs within the same cable); and making an accurate determination of the location of any faults. To obtain the foregoing "results", Harris clearly must determine whether or not there is an "equipment alarm", i.e., a physical alarm, not a logical alarm.

In col. 5, lines 37-39, Harris clearly discloses "the received alarms will identify the specific equipment reporting the alarm." Therefore, the alarm is a physical alarm, because it identifies a physical component of the system.

In col. 6, lines 45-65, Harris discusses Fig. 2C. Harris' discussion pertains to "los of signal"

(see line 56). As noted by the Applicant''s specification, a loss of signal is a physical error and therefore results in a physical alarm. It appears, albeit erroneously, from (c) on page 12 of the office action, that the Examiner wants to hold an alarm based on a loss of signal resulting in a transmission failure (step 231 of Fig. 2c) to be a physical alarm, and the alarm based on the loss of signal resulting in a reception failure (step 233) to be a logical alarm because of how these alarms are utilized/analyzed. However, since both are the result of a "loss of signal", then both must be physical alarms.

The Examiner should provide a reference that teaches that equipment alarms or hardware faults are known in the art to be logical errors/logical alarms, or withdraw the rejection.

For example, U.S. Patent No. 6,873,598 to Randall L. Powers, et al. titled Embedded Cell Loopback Method And System For Testing In ATM Networks (of record) describes a method and apparatus for testing components in ATM networks, and indicates that "if a *physical alarm* is active on any of the components through which the virtual channel passes . . . it is likely that the physical component problem is in fact causing the fault" (emphasis added). Accordingly, alarms generated based on faults of physical components in a network system are termed "physical alarms."

Accordingly, the rejection of claims 1 and 8 is deemed to be in error and should not be sustained.

Additionally, those features that rely in the foregoing step of *determining whether or not said alarm information corresponds to a logical alarm* , are also not taught by the applied art. For example, claims 1 and 8 call for *determining the location of the network element generating the*

alarm information, when it is determined that the alarm information is due to ***a logical error***. Since Harris does not make any determinations with respect to logical errors, then the foregoing feature of claims 1 and 8 are not taught by Harris. Joyce was not applied in this regard.

Accordingly, the rejection of claims 1 and 8 is deemed to be in error and should not be sustained.

Both claim 1 and claim 8 call for *increasing a count value representing a number of times in which the same alarm information has been generated, without redundantly storing said alarm information into said database, when it is determined that said alarm information is already stored in said database.*

In Harris' count process, each upstream trunk is processed in turn. On each trunk, a circuit alarm counter is incremented. The directionality of the circuit alarm with respect to the trunk is significant and separate counters are maintained for circuit alarms in each direction.

If the circuit alarm is the first alarm to be counted on a given trunk, or if the time-stamp of the alarm falls outside the window for presuming correlation with any previous alarms, then the time-stamp of that alarm and the set of all upstream trunks are stored in the data structure representing the trunk. Otherwise, if the circuit alarm is not the first one to be counted on a given trunk and the time-stamp of that alarm is within the window necessary for presuming correlation with the previous alarms, then the set of upstream trunks for the new alarm is intersected with that of the previous alarm or alarms (that is, all trunks common to both sets are extracted), and the new list is stored in the trunk data structure. This intersection set will be referred to as the "common path

set" for the circuits on the trunk: at any given time, this is the set of trunks that contain all of the same circuits as those counted on the given trunk. (This set always contains the given trunk itself, and it may contain only that trunk if the circuits do not have any other trunks in common.) <u>The significance of this common path set is that the circuit alarms counted on the given trunk could actually be caused by an outage **on any of these trunks.**</u>

Every time that a circuit alarm counter is incremented on a given trunk, then that trunk is evaluated to determine if a fault can be**inferred** from the circuit alarms or if a reported trunk fault can be confirmed to be affecting traffic on the contained circuits.

Accordingly, there is no determination as to whether the <u>*same alarm*</u> information has been generated. Harris clearly describes determinating whether "a fault can be inferred". The counter is incremented to record <u>**the number of systems associated**</u> with an outage, not to identify when *same alarm information* occurs more than once.

With respect to the above, the Examiner notes that Harris does not explicitly teach:

increasing a count value representing a number of times in which the same alarm information has been generated, without redundantly storing said alarm information into said database, when it is determined that said alarm information is already stored in said database; nor

storing the increased count value at a position corresponding to said alarm information already stored in said database.

Accordingly, the Examiner applies Joyce in this regard.

Joyce is related generally to minicomputer systems and more particularly to storage

hierarchies having high speed, low capacity storage devices and lower speed, high capacity storage devices coupled in common to a system bus. Joyce is not concerned with network telecommunications.

Accordingly, Joyce is **not analogous** to Harris not the present invention.

It appears, instead, that the Examiner found Harris to be lacking with respect to the foregoing features of claims 1 and 8, and based on this, *i.e.,* **hindsight**, sought out a system having a memory buffer and associated counter.

Joyce's system includes a number of counters and the Examiner refers us to one set forth in the last feature of claim 1:

> a counter coupled to said encoder and to said RAM circuits to increment by one said encoder output and store an incremented count in said column address of said RAM circuits for enabling the storing of information corresponding to said replacement information in the location of said data buffer identical of that stored in main memory during said replacement operation.

Joyce's counter is, therefore, an address counter that is incremented to allow for the storage of of replacement information. This counter is not incremented on the basis of finding that current information is the same as previously stored information such that the current information is not stored. Nor is the count incremented to indicate the number of times the information was stored, as Joyce's claim clearly describes incrementing the count to enable the storage of information corresponding to replacement information.

Accordingly, the rejection of claims 1 and 8 is deemed to be in error because Joyce does not teach the feature of *increasing a count value representing a number of times in which the same*

alarm information has been generated, without redundantly storing said alarm information into said database, when it is determined that said alarm information is already stored in said database , noted as lacking in Harris.

Accordingly, the rejection of claims 1-14 is deemed to be in error and should not be sustained.

Respectfully submitted,

Robert E. Bushnell,
Attorney for the Applicant
Registration No.: 27,774

1522 "K" Street N.W., Suite 300
Washington, D.C. 20005
(202) 408-9040

Folio: P56352
Date: 10/30/06
I.D.: REB/MP

VIII. APPENDIX

CLAIMS UNDER APPEAL

1. (Original) A method for managing alarm information in a network management system, comprising the steps of:

receiving alarm information generated from any of a plurality of network elements;

determining whether or not said alarm information corresponds to a logical alarm;

determining the location of the network element generating the alarm information, when it is determined that the alarm information corresponds to a logical alarm;

searching a database to determine whether said database already has said alarm information stored therein, according to the location of the network element generating the alarm information;

storing said alarm information when it is determined that said database does not have said alarm information already stored therein;

increasing a count value representing a number of times in which the same alarm information has been generated, without redundantly storing said alarm information into said database, when it is determined that said alarm information is already stored in said database; and

storing the increased count value at a position corresponding to said alarm information already stored in said database.

2. (Original) The method as set forth in claim 1, wherein the step of searching said database further comprises the steps of:

analyzing said alarm information to detect its positional value and event type; and

determining whether said database has the alarm information of the same positional value and event type.

3. (Original) The method as set forth in claim 1, wherein the step of searching said database further comprises the steps of:

detecting the positional value of said alarm information from its data format; and

identifying destination information by analyzing a virtual path identifier and a virtual channel identifier of subscriber connection information corresponding to the alarm location to determine an identity of a subscriber from which said alarm information was generated.

4. (Original) The method as set forth in claim 1, further comprising a step of parsing said alarm information for storage into said database when it is determined that the alarm information does not correspond to a logical alarm.

5. (Original) The method as set forth in claim 1, wherein said database comprises a plurality of network element tables, each corresponding to a respective one of said network elements, said step of storing further comprising storing said alarm information into the corresponding network element table of said database according to the location of the network element.

6. (Original) The method as set forth in claim 5, further comprising a step of converting

the alarm information through a database application interface into a database data format of said database to be recorded as new alarm information in the network element table of the network element generating the alarm information.

7. (Original) The method as set forth in claim 5, further comprising steps of:

displaying said alarm information stored in said database;

entering search parameters for finding a particular error corresponding to the alarm information or for finding a particular network element and its corresponding alarm information; and

displaying information retrieved as a result of said step of entering search parameters.

8. (Original) A method for managing alarm information in a network management system connected to a plurality of subscribers at a plurality of network elements, comprising the steps of:

driving an alarm daemon processor when said network management system is powered on;

receiving, via said alarm daemon processor, alarm information generated from at least one of said network elements;

determining whether said alarm information is due to a logical error or a physical error in the network element generating the received alarm information;

determining the location of the network element generating the alarm information, when it is determined that the alarm information is due to a logical error;

searching a database to determine whether said database already has said alarm information

stored therein, according to the location of the network element generating the alarm information;

storing said alarm information when it is determined that said database does not have said alarm information already stored therein;

increasing a count value representing a number of times in which the same alarm information has been generated, without redundantly storing said alarm information into said database, when it is determined that said alarm information is already stored in said database; and

storing the increased count value at a position corresponding to said alarm information already stored in said database.

9. (Original) The method as set forth in claim 8, wherein the step of searching said database further comprises the steps of:

analyzing said alarm information to detect its positional value and event type; and

determining whether said database has the alarm information of the same positional value and event type.

10. (Original) The method as set forth in claim 8, wherein the step of searching said database further comprises the steps of:

detecting the positional value of said alarm information from its data format; and

identifying destination information by analyzing a virtual path identifier and a virtual channel identifier of subscriber connection information corresponding to the alarm location to determine an identity of a subscriber from which said alarm information was generated.

11. (Original) The method as set forth in claim 8, further comprising a step of parsing said alarm information for storage into said database when it is determined that the alarm information is due to a physical error.

12. (Original) The method as set forth in claim 8, wherein said database comprises a plurality of network element tables, each corresponding to a respective one of said network elements, said step of storing further comprising storing said alarm information into the corresponding network element table of said database according to the location of the network element.

13. (Original) The method as set forth in claim 12, further comprising a step of converting the alarm information through a database application interface into a database data format of said database to be recorded as new alarm information in the network element table of the network element generating the alarm information.

14. (Original) The method as set forth in claim 12, further comprising steps of:

displaying said alarm information stored in said database;

entering search parameters for finding a particular error corresponding to the alarm information or for finding a particular network element and its corresponding alarm information; and

displaying information retrieved as a result of said step of entering search parameters.

IX. EVIDENCE APPENDIX

None.

X. RELATED PROCEEDINGS APPENDIX

None.